Hypergeometric series and elliptic curves over finite fields

AUTHOR(S):

小池, 正夫

CITATION:

小池, 正夫. Hypergeometric series and elliptic curves over finite fields. 数理解析研究所講究録 1993, 843: 27-35

ISSUE DATE:

1993-06

URL:

http://hdl.handle.net/2433/83584

数理解析研究所講究録
843巻 1993年 27-35

Hypergeometric series and elliptic curves over finite fields

広島大学理学部

小池 正夫

有限体上の超幾何関数は Gauss の和と Γ-関数の定義式の類似性に着目して、古典的な超幾何関数に対応する有限体上の対象として、Koblitz [3], Greene [2] によって定義され、研究が始められた。研究が始められてからまだ日も浅く重要な結果の数多くある数論の中で Gauss の和のような独自な位置をえられるかどうかは不確定だが、有限体上の超幾何多項式に新しい定義式をえたり、有限体上の代数曲線の研究に少しは新しい知識を加えることができると期待している。

$E_\lambda : y^2 = x(x-1)(x-\lambda)$ $\lambda \neq 0, 1 \in \mathbb{C}$ を Legendre の楕円曲線とすると

$$\int_1^\infty \frac{dx}{y} = \int_1^\infty \frac{dx}{\sqrt{x(x-1)(x-\lambda)}} = \pi\, {}_2F_1\left(\frac{1}{2}, \frac{1}{2}; 1; \lambda\right)$$

という等式が知られている。

ここで ${}_2F_1(a, b; c; x)$ は Gauss の超幾何級数で

$$ {}_2F_1\left(a,b;c;x\right) = \sum_{n=0}^{\infty} \frac{(a)_n (b)_n}{(1)_n (c)_n} x^n, \quad (a)_n = a(a+1)\cdots(a+n-1), $$

$(a)_0 = 1$

で定義されている。

一方 有限体上では 同じ形の楕円曲線

$$ E_\lambda : y^2 = x(x-1)(x-\lambda) \qquad \lambda \neq 0, 1 \in \mathbb{F}_p $$

の $\mathbb{F}_p$ 有理点の個数の計算が次の式で得られる:

$$ N_\lambda = 1 + \sum_{t \in \mathbb{F}_p} \left\{ 1 + \phi(t(t-1)(t-\lambda) \right\} $$

$$ = 1 + p + \sum_{t \in \mathbb{F}_p^\times} \phi(t)\phi(1-t)\phi(1-t\lambda) $$

ここで $\phi \in \widehat{\mathbb{F}_p^\times}$ は Legendre 指標で $\phi(0)=0$ とし $\mathbb{F}_p$ までのばして考えている。従って E_λ の合同ゼータ関数の分子に現れる Frobenius 写像の跡 $a_p(\lambda)$ は

$$ a_p(\lambda) = -\sum \phi(t)\phi(1-t)\phi(1-t\lambda) $$

とかけ、この右辺を有限体上の超幾何関数の定義式でおきかえると、

$$ a_p(\lambda) = -p\,\phi(-1)\,{}_2F_1\left(\begin{matrix}\phi & \phi \\ & \varepsilon\end{matrix} \middle| \lambda\right) $$

となる。ε は $\mathbb{F}_p^\times$ の単位指標を表す。これは $\mathbb{C}$ 上の楕円積分を超幾何関数でかいた式と類似している。

$a_p(\lambda) \pmod p$ は Deuring によれば ${}_2F_1\left(\frac{1}{2},\frac{1}{2};1;x\right)$ の係数を有限体の元とみて、分子が0になるところでとめて得られる λ の $\frac{p-1}{2}$ 次式の多項式（これを超幾何多項式

と呼ぶことにする.) で書くことは Manin による解釈が与えられている。(Clemens [1] を参照) しかし modulo p する前の等式は目新しい。

又 Legendre 型の楕円曲線について超幾何多項式との関係は Silverman [9], Clemens [1], Husemöller など詳しい解説をみるが、その他の楕円曲線の族についての記述は不勉強のせいもあるがすぐ目につかない。だから上の等式を拡張するような楕円曲線の族と超幾何関数の関係をかいておくのは無駄ではないだろう。

研究集会の折に、伊原先生が注意してくださったのは Dwork による p進的な超幾何関数の研究についてでした。

最近の Young [10] の結果によれば変数 $\widetilde{\lambda}$ を p進数で $\widetilde{\lambda}(\mathrm{mod}\, p) = \lambda$ でもって $a_p(\lambda)$ という Frobenius 写像の跡ではなくて、その Frobenius 写像の2つの固有値のうち p進単数が、p進的な超幾何関数の特殊値になっています。従って modulo p するとどちらも同じ式になるわけですが、両者の関係は注意されていないようです。Young [10] では [4] で示した Apéry 数の合同式も p進的な超幾何関数の研究の応用で得られている。この点でも両者が平行している。

§1 難波氏の実験

$a_p(\lambda)$ を上にのべた λ の関数として、この関数に次のように行列を対応させる。それは一般的に $f: \mathbb{F}_p^\times \to \mathbb{C}$ が与えられているとする。$\mathbb{F}_p^\times$ の生成元を r, $m = \frac{p-1}{2}$ として

$$c_i = f(r^i) - f(-r^i) \qquad 0 \le i \le m-1$$

とおいて m 行 m 列の行列 $\Phi = \Phi_f$ を

$$\Phi = \Phi_f = \begin{bmatrix} c_0 & c_1 & c_2 & \cdots & c_{m-1} \\ -c_{m-1} & c_0 & \ddots & & \\ -c_{m-2} & -c_{m-1} & \ddots & & \\ \vdots & \vdots & \ddots & & \\ -c_1 & -c_2 & \cdots & & c_0 \end{bmatrix}$$

で定義する。難波[7], [8]では $a_p(1)$ を適当に定義して、対応する行列 Φ の計算を素数 p を変えて数値実験の結果、次の予想を提出している。

予想 $\quad p \equiv 1 \pmod 4$ ならば $\quad {}^t\Phi \cdot \Phi = p^2 1_m$

$\quad p \equiv 3 \pmod 4$ $\quad {}^t\Phi \cdot \Phi = p^2 1_m - 2(p+1)\Omega$

ここで Ω は (i,j) 成分が $(-1)^{i+j}$ となる行列。

[7], [8]では他の超幾何関数の類似物についても同様の現象が得られることも予想されている。

§2 Mellin 変換

難波氏の行列を定義するのに §1 では有限体 $\mathbb{F}_p$ をとったが、任意の有限体 $\mathbb{F}$ $|\mathbb{F}| = q = p^\nu$ で同様の考察ができる。

$\mathbb{F}^\times$ の生成元を r とかいて、 $m = \frac{q-1}{2}$ とおく。関数 $f : \mathbb{F}^\times \to \mathbb{C}$ において $c_i = f(r^i) - f(-r^i)$, $0 \le i \le m-1$ とおいて m 行 m 列の行列 $\Theta = \Theta_f$ を同様に定義する。

一方、f の Mellin 変換 $M_f(\chi)$, $\chi \in \widehat{\mathbb{F}^\times}$ は

$$M_f(\chi) = \sum_{t \in \mathbb{F}^\times} \chi(t) f(t)$$

で定義する。

定理　次の2つの命題は同値である。

(A)　${}^t\overline{\Theta} \cdot \Theta = \alpha \cdot 1_m$

(B)　全ての奇指標 χ について　$M_f(\chi) M_f(\overline{\chi}) = \alpha$

ここで　$\chi(-1) = -1$ のとき χ を奇指標という。$\overline{\chi}$ は χ の複素共役で得られる指標を表す。

§3　有限体上の超幾何関数

性質(B)をみたす有限体上の関数の例として有限体上の超幾何関数から得られるものがある。有限体上には他に Hermite 多項式（Evans による）などあるが(B)を調べると成り立っていない。

有限体上の超幾何関数で Gauss の超幾何関数に対応するものは　$A, B, C \in \widehat{\mathbb{F}^\times}$ において　$x \in \mathbb{F}^\times$

$$ {}_2F_1\left(\begin{matrix}A, B\\ C\end{matrix}\middle| x\right) = \frac{BC(-1)}{q}\sum_{t\in F} B(t)\,\overline{BC}(1-t)\,\overline{A}(1-xt) $$

で定義される. ただし $A(0)=0$、$B(0)=0$ $C(0)=0$ とする. すると

この Fourier 展開は

$$ = \frac{q}{q-1}\sum_{\chi\in\hat{F}^\times}\binom{A\chi}{\chi}\binom{B\chi}{C\chi}\chi(x) $$

ここで $A, B\in\hat{F}^\times$ において $\binom{A}{B} = \frac{B(-1)}{q}J(A,\overline{B})$, Jacobi和

とする。 Mellin 変換と Fourier 変換の関係は明らかで、更に

それが簡単になる A, B, C の例としては.

$$ A=\psi,\quad B=\overline{\psi},\quad C=\varepsilon \qquad \psi\neq\varepsilon $$

が考えられ、そのとき

$$ M_f(\chi) = \binom{\chi}{\psi}\binom{\chi}{\overline{\psi}} $$

となる。これは Gauss 和でかき直して $G(\chi)G(\overline{\chi}) = \chi(-1)q$ を

用いると

補題 $\chi\neq\psi, \overline{\psi}, \varepsilon$ ならば $M_f(\chi)M_f(\overline{\chi}) = 1$

依って §2 の定理と合わせれば.

定理 ψ が自明でない偶指標とすると、 ${}_2F_1\left(\begin{matrix}\psi, \overline{\psi}\\ \varepsilon\end{matrix}\middle| x\right)$

からきまる行列重は.. 直交行列になる。

特に有限体 $\mathbb{F}_p$ で $\psi=\phi$ Legendre 指標のときが §1 の難波氏の

予想と関係していて、 $p\equiv 1 \pmod 4$ という条件は ϕ が

偶指標と同値だから予想の証明がえられる。 $p\equiv 3 \pmod 4$

の場合も §2の途中の計算をたどることで同様に得られる。

§4 楕円曲線の族と超幾何関数

解けている場合に限るために有限体を改めて $\mathbb{F}_p$ の場合とする。難波[7], [8]との関連から次の4つのCaseが次の対象として現れる。

Case 1	$p \equiv 1 \pmod 2$	$\psi = \omega^{\frac{p-1}{2}}$
Case 2	$p \equiv 1 \pmod 3$	$\psi = \omega^{\frac{p-1}{3}}$
Case 3	$p \equiv 1 \pmod 4$	$\psi = \omega^{\frac{p-1}{4}}$
Case 4	$p \equiv 1 \pmod 6$	$\psi = \omega^{\frac{p-1}{6}}$

ここで ω は Teichmüller 指標とする。

これら4つのCaseでは $-p\,{}_2F_1\left(\begin{matrix}\psi & \bar{\psi}\\ \varepsilon\end{matrix}\middle| x\right)$ に合同な行列 $\overline{F_f}$ は有理整数係数となっている。Case 1では楕円曲線 $y^2 = x(x-1)(x-\lambda)$ の $a_p(\lambda)$ と超幾何関数 ${}_2F_1\left(\begin{matrix}\phi & \phi\\ \varepsilon\end{matrix}\middle| \lambda\right)$ との関係式があったように、残りのCaseでも楕円曲線との関係が期待される。実際 Case 3, Case 4 については、次の結果が得られる。

定理 素数 $p \geq 101$ とする。楕円曲線 E_λ^2:

$$E_\lambda^2 : \quad y^2 = x^3 + x^2 + \frac{\lambda}{4}x \qquad \lambda \neq 0, 1$$

の Frobenius 写像の跡を $a_p(\lambda, 2)$ とおくと

$$a_p(\lambda, 2) = -p\,{}_2F_1\left(\begin{matrix}\psi & \bar{\psi}\\ \varepsilon\end{matrix}\middle| \lambda\right)$$

ただし ψ は Case 3 の指標。

定理 同じ p についての条件で 楕円曲線 E_λ^1

$$E_\lambda^1 : y^2 = x^3 + x^2 - \frac{4}{27}\lambda \qquad \lambda \neq 0, 1$$

の Frobenius 写像の跡 $a_p(\lambda, 1)$ について

$$a_p(\lambda, 1) = -p\, {}_2F_1\left(\psi, \frac{\overline{\psi}}{2} \middle| \lambda\right)$$

ただし ψ は Case 4 の指標

Case 2 の場合を残したのは 楕円曲線の族としては $x^3 + y^3 + z^3 = 3\mu xyz$ の Frobenius 写像の跡と関係することは 金子氏から教わったのだが、他の Case と違うところは関数の定義域が μ^3 のところと対応するところでしか等式が成立することが証明できない。

難波 [7] [8] では 楕円曲線の族から出発して予想を得ているので、上の定理のように有限体上の超幾何関数での関係式がいえれば、§3 の結果が使えて予想の証明ができる。だから 有限体上の超幾何関数との関係がわからない場合の予想は未だ解けていない。特に大きく残っているのは $p \equiv 2 \pmod 3$ の場合には 位数 3 の指標 ψ は $\widehat{\mathbb{F}_p^\times}$ には存在しない。ところが $a_p(\lambda)$ は定義できて、予想もある。

$p \equiv 3 \pmod 4$, $p \equiv 5 \pmod 6$ の場合も同様である。これらは有限体上の超幾何を使う証明は未だない。

References

[1] C.Clemens. A Scrapbook of Complex Curve Theory, Plenum Press, 1980.(Chapter 2).

[2] J.Greene, Hypergeometric functions over finite fields, Trans.A.M.S.,301,77-101,1987.

[3] N.Koblitz, The number of points of certain families of hypersurfacea over finite fields, Compositio Math., 48, 3-23, 1983.

[4] M.Koike, Hypergeometric series over finite fields and Apéry numbers, Hiroshima Math. J.,22, 461-467, 1992.

[5] M.Koike, Shift orthogonal matrices obtaines from hypergeometric series over finite fields and elliptic curves over finite fields, preprint.

[6] K.Namba, Legendre polynomial over finite fields and factorization of integers, Proc. Int. Symp., Hua Lookeng, Springer 1991.

[7] K.Namba, Elliptic curves over finite fields and cyclic rational orthogonal matrix, 応用数学合同研究集会　１９９０年

[8] K.Namba, Elliptic curves over finite fields and cyclotomic polynomials, 応用数学合同研究集会　１９９１年

[9] J. Silverman, The arithmetic of elliptic curves, GTM 106, Springer-Verlag,1986.

[10] P.T.Young,Apéry numbers,Jacobi sums, and special values of generalized p-adic hypergeometric functions, J.Number Theory,41,231-255,1992.